Department of Defense
DIRECTIVE

SUBJECT: Management of DoD Information Resources and Information Technology

References: (a) DoD Directive 7740.1, "DoD Information Resources Management Program," June 20, 1983 (hereby canceled)
    (b) DoD 7740.1-G, "Department of Defense ADP Internal Control Guideline," July 19, 1988 (hereby canceled)
    (c) DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992 (hereby canceled)
    (d) Public Law 104-13, "Paperwork Reduction Act" (Chapter 35 of title 44, United States Code)
    (e) through (n), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Cancels references (a) and (b).

1.2. Reissues reference (c) to implement references (d), (e), (f), (g), and (h).

1.3. Establishes policies for DoD information resources management (IRM), including information technology (IT), and delineates authorities, duties, and responsibilities for DoD IRM activities consistent with reference (i).

1.4. Provides direction on establishing Chief Information Officers (CIOs) at various levels consistent with reference (e).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. All phases and activities of the information life cycle regardless of medium or intended use within the Department.

2.1.3. All DoD IT, including IT in National Security Systems (NSS).

2.2. This Directive does not change or otherwise affect information release or disclosure requirements imposed by the Arms Export Control Act, the Privacy Act, the Freedom of Information Act, and Sections 2320 and 2321of title 10, United States Code.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Each DoD Component shall have a CIO who reports directly to the Head of the Component, and who shall head an office responsible for ensuring that the DoD Component complies with and promptly, efficiently, and effectively implements information policies and IRM responsibilities in this Directive.

4.2. CIOs may be designated at sub-Component levels.

4.3. Forums shall be established to:

4.3.1. Exchange views and solidify relationships between the DoD Component CIO, and the Joint Community CIO (reference (j)) and other senior managers (e.g., functional managers, Acquisition Executives, Comptrollers).

4.3.2. Identify and establish IRM best practices.

4.3.3. Resolve issues to effectively and efficiently manage information and the technology that supports it.

4.4. Accurate and consistent information shall be available to decision-makers so they can effectively execute the DoD mission. Accordingly:

4.4.1. The function or activity shall determine the need for and availability of information.

4.4.2. Data and information shall be structured to enable full interoperability and integration across DoD operations and activities. Creation of duplicate data shall be minimized and to the extent possible data shall be entered only once. This increases data accuracy, decreases the need for resources to reconcile data from several sources, and promotes data sharing.

4.4.3. An integrated DoD architecture with operational, system, and technical views shall be developed, maintained, and applied to determine interoperability and capability requirements, promote standards, accommodate the accessibility and usability requirements of reference (k), and implement security requirements across the DoD enterprise to provide the basis for efficient and effective acquisition and operation of IT capabilities.

4.4.4. Where workable and cost effective, the DoD Components shall use DoD-wide automated information systems (AIS) and software applications. These AIS shall be designed to use common or enterprise networks, data centers, computing hardware, and databases.

4.4.5. The DoD Components shall use a disciplined life-cycle approach to manage information resources from acquisition through retirement.

4.5. Integrated analysis, planning, budgeting, and evaluation processes shall strengthen the quality of decisions about using IT to meet mission needs. Accordingly:

4.5.1. Performance- and results-based management processes and tools shall guide IT investments and ensure they provide measurable improvements to mission performance. Key steps in implementing these management processes and tools include the following:

4.5.1.1. IRM strategic plans that horizontally and vertically integrate information resources activities throughout the Department, and align IT investments to mission-related outcomes.

4.5.1.2. The Planning, Programming, and Budgeting System (PPBS) and Defense Acquisition System (DAS) processes used as the capital planning and investment control process for maximizing the value and assessing and managing the risks of IT investments.

4.5.1.3 Measurements of performance to gauge progress in achieving IT performance goals.

4.5.1.4. Practices that base decision-making on performance information.

4.5.2. Criteria related to the quantitatively expressed projected net risk-adjusted return on investment and specific quantitative and qualitative criteria shall be used to compare and prioritize alternative IT investment projects.

4.6. Before applying IT:

4.6.1. The DoD Components shall determine whether the functions that IT will support are central to or priorities for the Department's mission. The DoD Strategic Plan, required by reference (l), shall be the bases for identifying:

4.6.1.1. The Department's core mission, priorities, goals, and objectives, and how they will be achieved and measured.

4.6.1.2. What the function contributes to the DoD Strategic Plan and warfighter and customer requirements. The DoD Components shall determine whether the private sector or another Government Agency can perform the particular function more effectively and at less cost.

4.6.2. The DoD Components shall outsource non-core and inherently non-governmental functions to another Government Agency or the private sector when it makes good business sense to do so.

4.6.3. The DoD Components shall routinely and systematically benchmark their functional processes against models of excellence in the public and private sectors. Maximum use shall be made of commercial-off-the-shelf (COTS) and non-developmental item (NDI) products and services when refining, reengineering or redesigning functional processes. Benchmarks and associated analyses, as well as business reengineering practices, methodologies and tools shall be employed by the DoD Components to develop, simplify or refine functional processes before IT solutions are applied.

4.6.4. Information assurance requirements shall be identified by the DoD Components during functional process reengineering, and/or outsourcing.

4.7. Acquisition strategies shall:

4.7.1. Appropriately allocate risk between the Government and a contractor.

4.7.2. Effectively use competition.

4.7.3. Tie contractor payments to performance.

4.7.4. Take maximum advantage of COTS.

4.8. To reduce risks while speeding the delivery of IT capabilities, the DoD Components shall base decisions to develop and modernize IT on the following:

4.8.1. Accurate, detailed descriptions of customer requirements and specifications, and related performance measures that can be used during testing, shall drive the design, development, and support of IT.

4.8.2. Early involvement, buy-in, and feedback from customers/users shall continue throughout the IT project.

4.8.3. Phased, evolutionary IT-acquisition segments that are as brief and narrow in scope as possible. Each segment shall solve a specific part of an overall mission problem and deliver a measurable net benefit independent of future segments.

4.8.4. IT shall be shared and reused wherever possible.

4.8.5. Commercial or NDI shall be used as much as possible, while custom-designed components shall be avoided or isolated to minimize the potential adverse consequences on the overall project.

4.8.6. Initial information system designs shall integrate information assurance components to ensure they provide reliable, timely, and accurate information that is protected, secure, and resilient against information warfare, terrorist, and criminal activities.

4.8.7. Pilots, models, simulations, and prototypes shall be encouraged to gain early insights into required IT capabilities. However, IT capabilities shall be fully tested before going into production.

4.8.8. The DoD Components shall establish and track clear goals (e.g., cost, schedule, and performance), measures, and accountability for IT project progress so that the Component can correct problems quickly as they arise.

4.9. Programs shall be established to acquire, develop, and retain a well-trained core of highly qualified IRM and information assurance professionals who can accept, anticipate, and generate the changes that IT will enable.

4.10. Disabled DoD employees or members of the public seeking information or services from the Department of Defense shall have access to and use of information and data comparable to the access and use by individuals who are not disabled, unless an undue burden would be imposed (reference (k)).

5. REPONSIBILITIES

     5.1. The Assistant Secretary of Defense for *Networks and Information Integration*, as the DoD Chief Information Officer, shall:

          5.1.1. Serve as the Principal Staff Assistant for information resources management matters related to references (d) through (i).

          5.1.2. Participate in the PPBS process and advise the Secretary and Deputy Secretary of Defense, and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) on major resource allocation and investment decisions, including recommending whether to continue, modify, or terminate IT investments.

          5.1.3. Serve on the Defense Acquisition Board, and advise the USD(AT&L) on IT opportunities and issues related to Defense Acquisition Programs.

          5.1.4. Chair the DoD CIO Executive Board (reference (m)), which shall serve as the principal DoD advisory body on matters pertaining to references (d) through (i).

          5.1.5. Serve as the DoD primary representative to Federal and interagency bodies supporting Federal IT policies.

          5.1.6. Chair the Architecture Coordination Council with the USD(AT&L) and the Joint Community CIO (reference (j)), to synchronize the Department's architectural activities and establish DoD architectural guidance.

          5.1.7. Issue enterprise-wide plans, policies, and procedures that enable the DoD Components to effectively and efficiently manage information resources, including IT, to achieve the Department of Defense's strategic goals.

          5.1.8. Promote improvements to DoD work processes and supportive information resources according to reference (i). This shall include developing, maintaining, and issuing guidance on functional process improvement methodologies and their supporting suite of procedures and tools.

          5.1.9. Design and implement, with the DoD PPBS and DAS authorities, a process for maximizing the value, and assessing and managing the risks of DoD IT acquisitions.

          5.1.10. Institutionalize performance- and results-based management for information resources, including IT, in coordination with the DoD Chief Financial Officer (CFO), the USD(AT&L), and the DoD Component CIOs.

5.1.11. Monitor and evaluate the performance of Major Automated Information Systems and other DoD IT programs that are of special interest to the Department of Defense, and advise the Secretary and Deputy Secretary of Defense, and the USD(AT&L) on whether to continue, modify, or terminate a program.

5.1.12. Develop, maintain, and facilitate, with the Chairman of the Joint Chiefs of Staff and the USD(AT&L), the implementation of a sound and integrated IT architecture for IT programs, including NSS, that will increase the value of the Department's information resources.

5.1.13. Establish information assurance policies and procedures that allow the DoD Components to exchange and use information securely meeting both warfighting and business requirements.

5.1.14. Perform the following according to reference (h):

5.1.14.1. Review and provide recommendations to the Secretary and Deputy Secretary of Defense, and the USD(AT&L) on DoD budget requests for IT, including NSS.

5.1.14.2. Ensure the interoperability of IT, including NSS, throughout the Department of Defense.

5.1.14.3. Ensure that IT, including NSS, standards that will apply throughout the Department of Defense are prescribed.

5.1.14.4. Institute policies and procedures that provide for the elimination of unnecessarily duplicative IT within the DoD Components and between each other.

5.1.15. Establish policies, programs, and initiatives with the Under Secretary of Defense (Personnel and Readiness) and the USD(AT&L) to strengthen DoD personnel's ability to manage information resources effectively.

5.1.16. Implement, monitor, and guide the use of COTS and NDI capabilities, with the USD(AT&L), as part of the DoD IT architecture.

5.1.17. Ensure that the IT standards of reference (k) are met.

5.2. The <u>Under Secretary of Defense for Acquisition, Technology, and Logistics</u> shall:

5.2.1. Consistent with reference (n), ensure that, where possible, the DoD Acquisition System's process for acquiring IT is simple, clear, and understandable, and specifically addresses managing risk, evolutionary or spiral acquisitions, and incorporating IT in a timely manner.

5.2.2. Chair the Defense Acquisition Board.

5.2.3. Chair the Architecture Coordination Council with the DoD CIO and the Joint Community CIO (reference (j)), to synchronize the Department's architectural activities and establish DoD architectural guidance.

5.2.4. Institutionalize performance- and results-based management for information resources, including IT, in coordination with the DoD CIO, the DoD CFO, and the DoD Component CIOs.

5.2.5. Support the development of systems views to develop, maintain, and facilitate the implementation of a sound and integrated IT architecture for IT programs, including NSS, that will increase the value of the Department's information resources in coordination with the Chairman of the Joint Chiefs of Staff and the DoD CIO.

5.2.6. Support and participate in the Chairman of the Joint Chiefs of Staff Requirements Generation System and DoD Component planning to ensure that acquisition reforms and interoperability requirements are visible in warfighting operations and to support seamless transitions between peace and war.

5.3. The <u>Under Secretary of Defense (Comptroller)/Chief Financial Officer</u> shall:

5.3.1. Develop and maintain the DoD Strategic Plan consistent with reference (l).

5.3.2. Establish policies and procedures to ensure that accounting, financial, and asset management, and other related DoD IT systems are designed, developed, maintained, and used effectively by the DoD Components to provide financial data reliably, consistently and expeditiously, and support programmatic IT investment decisions.

5.4. The <u>OSD Principal Staff Assistants</u> shall, according to their responsibility and authority for assigned functional areas, including the supporting information systems (ISs):

5.4.1. Improve DoD operations and procedures by ensuring the application of sound business practices, and compliance with this Directive.

5.4.2. Implement, execute, and exercise oversight for the evaluation and improvement of functional processes, as well as the development of functional process performance measures and assessments.

5.4.3. Develop, integrate, implement, and maintain functional strategic plans, objectives, operational and system architectural views, IS strategies, and related models and repository contents that support the functional missions.

5.4.4. Promote commonality and interoperability of functional processes across the DoD Components; resolve functional issues affecting information resources management; and provide resolution for technical ISs integration issues in their functional areas.

5.4.5. Ensure that economic analyses are prepared and validated, as required.

5.4.6. Perform functional management control and oversight of their supporting IS, and ensure functional leadership throughout the systems' life-cycle phases.

5.4.7. Review funding requirements for information resources management and IT programs during PPBS activities and recommend appropriate adjustments and allocations.

5.4.8. Perform the following tasks:

5.4.8.1. Designate the DoD-wide automated information systems and applications to support activities and processes that fall within their functional areas.

5.4.8.2. Evolve DoD-wide automated information system and application investments as rapidly as possible for all DoD Components that perform the functional activity.

5.4.8.3. Identify and recommend termination of other automated information systems and applications performing the functional activity.

5.5. The Chairman of the Joint Chiefs of Staff shall:

5.5.1. Appoint a Joint Community CIO, consistent with reference (j).

5.5.2. Improve operations and procedures under his purview by ensuring the application of sound business practices, and compliance with this policy guidance.

5.5.3. Support and participate in functional/business area and DoD Component planning to ensure that the Chairman of the Joint Chiefs of Staff and Commanders-in-Chief requirements for warfighting operations are visible and to support seamless transitions between peace and war.

5.5.4. Validate the linkage of IT support to the joint information requirements of the warfighters.

5.5.5. Perform the following tasks:

5.5.5.1. Designate the joint automated information systems and applications that will be used to support activities and processes that warfighters require.

5.5.5.2. Evolve, with the DoD Components, each joint automated information system and application investment as rapidly as possible for all DoD Components that perform that activity.

5.5.5.3. Identify and recommend termination of other automated information system and application investments performing the activity.

5.6. The <u>Heads of the DoD Components</u> shall:

5.6.1. Appoint the DoD Component CIO who shall have core knowledge, skills, abilities, and experiences to carry out the requirements of references (d) through (i).

5.6.2. Clearly delineate the DoD Component CIO's IRM role, responsibilities, and authority vis-È-vis those of the DoD Component Comptroller, the Component Acquisition Executive or a similar position, mission/functional area managers, and sub-Component-level CIOs.

5.6.3. Take advantage of the opportunities that IT can provide and ensure that the IT infrastructure will support mission and business strategies by positioning the DoD Component CIO to participate in the Component's long-range strategic planning.

5.6.4. Periodically conduct meetings with the CIO, Comptroller, Component Acquisition Executive or similar position, as well as other key senior managers to promote and forge a strong partnership among them in making strategic Component decisions.

5.6.5. Designate, or authorize the designation of, subordinate-level CIOs as needed.

5.7. The <u>DoD Component Chief Information Officer</u> shall:

5.7.1. Ensure compliance with this Directive and the requirements of references (d) through (i) within the DoD Component.

5.7.2. Provide advice and other assistance to the Component Head and other Component senior management personnel to ensure that information resources are acquired, used, and managed by the DoD Component according to references (d) and (i).

5.7.3. Advise the DoD CIO and implement his or her policies and guidance.

5.7.4. Validate the linkage of Component IT support to the requirements of the warfighters.

5.7.5. Support the selection and implementation of DoD-wide automated information systems and applications in the Component.

5.7.6. Ensure compliance with the standards of reference (k).

6. <u>EFFECTIVE DATE</u>

This Directive is effective immediately.

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
   E1. References, continued
   E2. Definitions

E1. <u>ENCLOSURE 1</u>

<u>REFERENCES</u>, continued

(e) Public Law 104-106, "Division E of the Clinger-Cohen Act of 1996"
(f) Executive Order 13011, "Federal Information Technology," July 16, 1996
(g) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," February 8, 1996
(h) Section 2223 of title 10, United States Code
(i) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," June 2, 1997
(j) Chairman of the Joint Chiefs of Staff Instruction 8010.01, "Joint Community Chief Information Officer," July 7, 2000
(k) Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d)
(l) Section 4(b) of Public Law 103-62, 31 U.S.C. 1115, "Government Performance and Results Act of 1993"
(m) DoD Chief Information Officer Executive Board Charter, March 31, 2000
(n) Federal Acquisition Streamlining Act of 1994

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. <u>Information</u>. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

E2.1.2. <u>Information Assurance</u>. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.3. <u>Information Life Cycle</u>. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

E2.1.4. <u>Information Management</u> (IM). The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

E2.1.5. <u>Information Resources</u>. Information and related resources, such as personnel, equipment, funds, and information technology.

E2.1.6. <u>Information Resources Management</u> (IRM). The process of managing information resources to accomplish Agency missions and to improve Agency performance, including through the reduction of information collection burdens on the public.

E2.1.7. <u>Information System</u>. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

E2.1.8. <u>Information Technology</u> (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that:

E2.1.8.1. Requires the use of such equipment; or

E2.1.8.2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E2.1.9. National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

E2.1.9.1. Involves intelligence activities.

E2.1.9.2. Involves cryptologic activities related to national security.

E2.1.9.3. Involves command and control of military forces.

E2.1.9.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.9.5. Is critical to the direct fulfillment of military or intelligence missions.[1]

---

[1] This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).